Altiris™ Patch Management Solution for Linux® 7.1 SP2 from Symantec™ Release Notes

Altiris™ Patch Management Solution for Linux® 7.1 SP2 from Symantec™ Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Altiris™ Patch Management Solution for Linux® 7.1 SP2 from Symantec™ Release Notes

This document includes the following topics:

About Patch Management Solution for Linux

Altiris Patch Management Solution for Linux from Symantec lets you scan Red Hat and SUSE Linux computers for security vulnerabilities, report on the findings, and automate the downloading and distribution of needed errata or software updates. This solution downloads the required patches and provides wizards to help you deploy them. During configuration, you can set up an automatic patch update schedule to ensure that managed computers are up-to date and protected on an ongoing basis.

Patch Management Solution for Linux is installed with and uses the same license as Patch Management Solution for Windows.

For more information, see the *Patch Management Solution for Windows 7.1 SP2 Release Notes* at the following URL:

http://www.symantec.com/docs/DOC4815

Patch Management Solution for Linux is a component of Patch Management Solution. When you install Patch Management Solution using Symantec Installation Manager, the following components are installed:

- Patch Management Solution for Windows
- Patch Management Solution for Linux
- Patch Management Solution for Mac

Patch Management Solution is part of the following suites:

- Altiris Client Management Suite from Symantec
- Altiris Server Management Suite from Symantec
- Altiris IT Management Suite from Symantec

What's new in Patch Management Solution for Linux 7.1 SP2

In the 7.1 SP2 release of Patch Management Solution for Linux, the following new features are introduced:

- Support for Red Hat Enterprise Linux 6.0 and 6.1, all variants
- Support for SUSE Linux Enterprise Server and SUSE Linux Enterprise Desktop version 11 SP1
- Performance and reliability improvements

General installation and upgrade information

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *Installing IT Management Suite* chapter in the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See the product's documentation for information on how to configure and use it.

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Install New Products**, and then choose to install this product. Do not use the **Install Product Updates** page to upgrade.

Symantec recommends that you upgrade all of the installed products to the latest version. The easiest way to achieve this is to choose to install a suite.

If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For additional information about upgrading, see the **Upgrading to IT Management Suite 7.1 SP2 - Best Practices** article at the following URL:

http://www.symantec.com/docs/TECH177513

After you upgrade the product, you must upgrade the Symantec Management Agent and the plug-ins that are installed on the managed computers. Symantec recommends that you do the following:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4743

System requirements

Patch Management Solution for Linux requires the following software to be installed:

- Symantec Management Platform 7.1 SP2
  Symantec Management Platform is installed or upgraded automatically when you use Symantec Installation Manager to install or upgrade this product.

See "Platforms supported by Patch Management Solution for Linux" on page 6.

Platforms supported by Patch Management Solution for Linux

The Patch Management Solution for Linux component of Patch Management Solution supports the following operating systems:

- SUSE Linux Enterprise Server 10, 10 SP1-SP4, x86, x86_64
- SUSE Linux Enterprise Server 11, 11 SP1, x86, x86_64
- SUSE Linux Enterprise Desktop 10, 10 SP1-SP4, x86, x86_64
- SUSE Linux Enterprise Desktop 11, 11 SP1, x86, x86_64
- Red Hat Enterprise Linux AS/WS/ES 4 x86, x86_64
- Red Hat Enterprise Linux Server/Desktop 5 x86, x86_64
- Red Hat Enterprise Linux Server/Workstation/Client 6.0, 6.1, x86, x86_64

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 1-1 on page 7.
- Hierarchy and replication issues
  See Table 1-2 on page 8.
- Other known issues
  See Table 1-3 on page 10.

Table 1-1 Installation and upgrade issues

Issue	Description	Article Link
Steps to do after migrating from 7.0.	■ Type the Novell Mirror Credentials on the **Novell Patch Remediation Settings** page. Starting from version 7.1, Patch Management Solution for Linux uses Novell Mirror Credentials to manage SUSE Linux updates. ■ Because of the changes in the architecture, it is not possible to migrate the selected software channels from 7.0 to 7.1 SP2. After you migrate the solution from 7.0 to 7.1 SP2, import the channels list and select the channels for which you want to download updates. ■ For Red Hat, after you upgrade the product, on the **Import Patch Data for Red Hat** page, select and import the same channels as you had in the 7.0 version of the product. If you do not import these channels, it is not possible to distribute migrated Red Hat packages. For more information, see the *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL: http://www.symantec.com/docs/DOC4743	DOC4743
Steps to do after upgrading from 7.1 and 7.1 SP1.	Run the **Import Patch Data for Novell** and **Import Patch Data for Red Hat** tasks.	
Breaking hierarchy before migrating to 7.1 SP2.	You must break the hierarchy if you are performing a migration from 7.0 to 7.1 SP2. After you break the hierarchy on the parent Notification Server computer, sometimes the child Notification Server computer retains its association with the parent server. Workaround: Also break the hierarchy on the child Notification Server computer.	

Table 1-1 Installation and upgrade issues *(continued)*

Issue	Description	Article Link
Invalid custom severities are not removed from the bulletins.	Invalid custom severities are cleaned up during upgrade. However, bulletins keep the invalid severities assigned to them. To remove an invalid severity from a bulletin, change its severity by using the right-click menu.	
Package server settings are not migrated from 7.0.	Package server settings on the **Policy and Package Settings** tab are not migrated from 7.0. Configure the settings after the migration.	
SQL queries in automation policies are overwritten.	Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	
Old server name is displayed in the **Compliance summary** report after the upgrade.	After the migration from 7.0, the old Notification Server computer's name is displayed in the **Compliance summary** report.	
Software Update Plug-in policies settings are not migrated.	The settings in the Software Update Plug-in Install, Uninstall, and Upgrade policies are not migrated from 7.x to this version of Patch Management Solution for Linux.	
Software Update policy targets are not migrated from 7.0.	The targets in the **Applied to** section are reset after migration. The targets are reset to the target value that is indicated in the **Default Software Update Plug-in Settings** policy.	
Custom severity with non-Latin characters is not migrated after upgrade from 7.0.	Sometimes custom severity with non-Latin characters is not migrated.	
RHEL3 and SLES9 are no longer supported.	The historical data is kept in the database, but you cannot download or install patches for RHEL3 and SLES9 after the migration.	

Table 1-2 Hierarchy and replication issues

Issue	Description	Article Link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217

Table 1-2 Hierarchy and replication issues *(continued)*

Issue	Description	Article Link
Software update policies on the child are not revised.	Software update policies that were created on child are not revised when you run the **Import Patch Data for Windows** task with the **Automatically revise Software Update policies after importing patch data** option checked on the parent Notification Server computer. Workaround: After the patch management import data replication is complete, recreate the policies on child using the same bulletins.	
An issue with default replication schedules.	There can be issues with data replication if all three replication rules (Windows, Novell, and Red Hat) run at the same time, which is 11:00PM by default. Symantec recommends that you stagger the replication schedules if you want to use both Windows and Linux patch management functionality in a hierarchy.	
Scheduled client tasks are not replicated to child immediately.	When you create a schedule for a client task (for example, **Run System Assessment Scan on Linux Computers**), and include managed computers from a child into the target, the schedule does not replicate to the child Notification Server computers immediately. Workaround: Use the **Run now** option.	
Exporting software update policies from parent to child is not supported.	Do not attempt to export a software update policy on the parent Notification Server computer and import it on the child. Instead use the built-in replication functionality.	
An issue with **Allow Package Server Distribution with Manual Prestaging** setting.	The **Allow Package Server Distribution with Manual Prestaging** settings are replicated, but displayed incorrectly in the Symantec Management Console of the child Notification Server computer. The functionality is not affected, you can ignore this user interface issue.	
Reports do not display any data from hierarchy.	With the exception of the **Compliance Summary** report, Patch Management Solution reports do not display any data from the child Notification Server computers. Only the data for the current Notification Server computer is displayed in patch reports.	
Packages are not replicated to child.	Child Notification Server computers download packages from Novell and Red Hat servers after the Patch metadata is replicated down the hierarchy.	

Table 1-2 Hierarchy and replication issues *(continued)*

Issue	Description	Article Link
Replicating data between different versions of Patch Management Solution is not supported.	Although some items may replicate between different versions of Patch Management Solution that are installed on parent and child Notification Server computers, Symantec does not recommend doing this. If you want to use hierarchy and replication, Patch Management Solution versions must be the same on the parent and child.	

Table 1-3 Other known issues

Issue	Description	Article Link
Relocating packages from an UNC location to another location does not work.	If on the **Core Services** page, you change the **To Location** value from an UNC path to another path, the packages will not be relocated. Workaround: Relocate the packages manually.	
Software updates cannot be downloaded from an alternate download location on a non-IIS package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	
Sometimes policy schedules work incorrectly across timezones.	Sometimes, when you create a schedule for a policy and select either **Use Agent time** or **Use Server time**, the policy does not run as planned on the endpoints that are located in a different time zone. Workaround: Use the **Coordinate using UTC** option.	
The **Terminate after** setting on the **Novell** and **Red Hat** pages does not work.	On the **Programs** tab on the **Novell** and **Red Hat** pages, when you set a value in **Terminate after**, the setting does not work. The default value of 60 minutes is always used.	
Staging Red Hat and Novell patches from an alternate location is not possible.	When you specify an alternate download location for Red Hat and Novell patches, the download fails. This setting is under **Settings > Software > Patch Management**, on the **Core Services** page, on the **Languages and Locations** tab.	

Table 1-3 Other known issues *(continued)*

Issue	Description	Article Link
The Patch Administrator cannot edit the default targets in the patch management configuration policies.	A user who belongs to the **Patch Management Administrators** role cannot edit default targets in the following policies: ■ Novell patch management configuration policy You access this policy from **Settings > Software > Patch Management > Novell Settings > Novell**. ■ Red Hat patch management configuration policy You access this policy from **Settings > Software > Patch Management > Red Hat Settings > Red Hat**. Workaround: On the configuration policy's page, delete the default targets, and then add the appropriate custom targets.	
Task details do not show the cause of the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** failing due to lack of free space on the Notification Server computer.	When there is no free space on the Notification Server computer, the **Import Patch Data for Red Hat** and **Import Patch Data for Novell** fail. When you open the task details in the **Task Status** table, no mention is made of the lack of free space causing the task to fail.	
Software updates import task status is incorrect.	When the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** task is running, the **Pending** status is displayed in the **Task Status** section of the task page. This status is not correct. To view the correct status of the task, click the task instance and open the task instance details.	
Software update details page does not work.	In Resource Manager, the **Summaries > Software Bulletin Details or Summaries > Software Update Details** pages do not work.	
The **Software Update Tasks Delivery Summary** Web part shows executed tasks as incomplete.	In the **Red Hat/Novell Software Update Tasks Delivery Summary** Web part, the tasks that were executed more than 30 days ago are shown as Incomplete.	
Reports can show incorrect data.	The **Novell/Red Hat Compliance by Update** report can show incorrect number of computers on which updates have been installed. For example, this happens when the same update belongs to two different channels. Such an update is displayed as if it was installed on two computers. To work around this issue, use the report's parameters section to filter the results by operating system or by software channel.	

Table 1-3 Other known issues *(continued)*

Issue	Description	Article Link
Cannot save settings on **Red Hat** and **Novell** pages when credentials left empty.	The changes on the **Red Hat** and **Novell** pages cannot be saved if you leave the credentials fields empty. Workaround: Type the credentials; the credentials are critical for the solution to work. If you do not know the valid credentials at the time of editing the configuration settings, you can type fake credentials.	
Sometimes policies with custom schedules can trigger other policies.	When you set a custom installation schedule for a policy, other policies with default schedules can also be triggered on the client computers and software updates will be installed. Other policies that have a custom schedule set are not affected by this issue. They will run on their scheduled time.	
Patch Management Solution for Linux cannot check for second-level dependencies.	Sometimes a software update cannot be installed because a dependency that was added to the policy is dependent on other software. Currently, Patch Management Solution for Linux does not run a dependency check for dependent software. Workaround: Add dependent packages to the policy manually.	
Sometimes a software update policy fails to save.	This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	
The **Software Bulletin Details** report shows the computers that are out of scope of the current console user.	In the **Software Bulletin Details** report, **Applies To** column, the number of all applicable computers is shown, including those for which the current console user has access and those for which access is disabled.	
Software update installations that require a computer restart are shown as complete.	The **Linux Software Update Delivery Summary** report shows software update installations that require computer restart as complete. You can use the **Restart Status** report to view if any computers are pending restart.	
Automation policy report **Maintain Retired Machine Historical Data** does not return any result.	The automation policy creates a report, but it contains no data.	

Table 1-3 Other known issues *(continued)*

Issue	Description	Article Link
Steps to do if installation fails.	Sometimes bulletin can fail to install because of a conflicting bulletin included into the same software update policy. To work around this issue, Symantec recommends that you create a software update policy for this failing bulletin only. If it still fails, you can set the log level to DEVNOTE and examine the rpm output. You can also try to install the update and its dependencies manually.	

Fixed issues

The following are the previous issues that were fixed in this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-4 Fixed issues

Issue	Description	Article Link
Software channels from multiple child servers are excluded from replication.	Because software channel resources from different child servers do not merge, only one child Notification Server computer per one parent Notification Server computer is supported for Patch Linux hierarchy.	
Bulletins that contain updates for different operating system versions cannot be distributed to the endpoints of child Notification Server computers, in case not all of the operating systems exist on the child.	This issue occurs when Inventory Solution is installed. Inventory Solution's **Software Products and metering/track usage configuration for the products** rule incorrectly replicates Patch Management Solution data to the child Notification Server computers. This results in inconsistent patch management data on the child. In this situation, the following errors occur: ■ In the **Linux Software Update Delivery Summary** report, failed policies have the status of **Policy Execution Incomplete**. ■ If Hierarchy Editable Properties are enabled, the **Policy reconstruction failed** error is displayed on the child Notification Server computer when you try to modify the policy. Workaround: To avoid this problem, make sure that all the child Notification Server computers that belong to the hierarchy have clients with the same collection of Red Hat operating system versions installed.	

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-5 Other things to know

Issue	Description	Article Link
You can use the First Time Setup portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP Server Settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next panel, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	
Updates download URLs for Novell and Red Hat.	The software updates metadata is downloaded from the following URLs: ■ Red Hat – http://xmlrpc.rhn.redhat.com ■ Novell – https://nu.novell.com Make sure that your firewall and proxy configuration allows network communication to these URLs.	

Table 1-5 Other things to know *(continued)*

Issue	Description	Article Link
Entitlement check is removed from the product.	Patch Management Solution for Linux no longer checks for entitlement. For this reason, inventory policies and the Update Agent Discovery task are removed from the product.	
Use mirror credentials for Novell.	In the previous versions of Patch Management Solution for Linux, you used Novell Customer Center credentials. Starting from version 7.1, you must type the Novell Mirror credentials on the **Novell** page, **Novell Customer Center** tab.	
Log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is `swuagent/var/InstallLog.txt`	
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	
Patch Management Solution for Linux creates a new Software association type during Patch data import	This is done for binding Linux update channels with exact OS version. This is working as designed.	HOWTO65658

Documentation that is installed

Table 1-6 Documentation that is included in the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. To open context-sensitive help, click inside the window, pane, dialog box, or other screen element about which you want more information, and then do one of the following: ■ Press the F1 key. ■ In the Symantec Management Console, click **Help > Context**. In the **Symantec Help Center** window, type your search string to search within the installed documentation. To expand your search to the Symantec Knowledge Base, check **Include online search**. For more information on how to use the **Symantec Help Center**, click the **Home** symbol.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/ business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Other information

Table 1-7 Information resources that you can use to get more information

Document	Description	Location
ITMS 7.1 SP2 Planning and Implementation Guide	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	http://www.symantec.com/docs/DOC4827

Table 1-7 Information resources that you can use to get more information *(continued)*

Document	Description	Location
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://www.symantec.com/docs/DOC4798
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page